JOURNAL OF NUMBER THEORY 16, 31–48 (1983)

Characters and Decomposition of a Representation in a Number Field

JOSEPH LEWITTES

Lehman College, Bronx, New York 10468, and the Graduate School, The City University of New York, 33 West 42 Street, New York, New York 10036

Communicated by H. Zassenhaus

Received January 21, 1981; revised May 17, 1982

Let A be an ideal in R, the ring of algebraic integers in a number field. The group of residue classes mod A prime to A has a representation U on the space of functions on $R \bmod A$. This representation is decomposed and the multiplicity of each character in it is determined. Some consequences of this are obtained and $\det U$ is evaluated.

1. INTRODUCTION AND PRELIMINARIES

Let R be the ring of algebraic integers in an algebraic number field K and A an integral ideal. Let $L(A)$ be the set of complex valued functions on the residue class ring $R \bmod A$; equivalently $f \in L(A)$ will be understood as a function on R having the elements of A as periods: $f(x+u) = f(x)$ for all $x \in R$, $u \in A$. N denotes the norm, NA is the number of elements in $R \bmod A$. $L(A)$ is a complex vector space of dimension NA, a basis being the set of functions $\{\delta_x\}_{x \bmod A}$—the notation indicating that x ranges over a set of representatives of $R \bmod A$—where $\delta_x(y) = 1$ if $y \equiv x \bmod A$ and $\delta_x(y) = 0$ otherwise. $L(A)$ becomes a finite dimensional Hilbert space with the inner product

$$(f, g)_A = \frac{1}{\sqrt{NA}} \sum_{x \bmod A} f(x)\,\overline{g(x)}. \tag{1}$$

If $r \in R$ is relatively prime to A the operator $U_r : L(A) \to L(A)$ defined by $U_r f(x) = f(rx)$ is easily seen to be well-defined, linear, unitary and depends only on $r \bmod A$. If also $s \in R$ is prime to A then $U_{rs} = U_r U_s$. Let $G(A)$ be the multiplicative group of residue classes of $R \bmod A$ that are prime to A. The map $r \bmod A \to U_r$ defines a unitary representation U of $G(A)$ on $L(A)$. The problem considered in this paper is the decomposition of U into a sum of irreducible representations. Since $G(A)$ is abelian the irreducible represen-

0022-314X/83/010031-18$03.00/0

641/16/1-3

tations are just the characters of $G(A)$. The main result (Theorem 3) is that each character χ occurs in U with multiplicity equal to the number of divisors of $A/M(\chi)$, where $M(\chi)$ is the conductor of χ.

In the remainder of this Introduction we fix notation and make some preliminary observations about U. Section 2 discusses characters and includes a count of real primitive characters of $G(A)$. Section 3 defines the operators I, J from $L(B) \to L(A)$, when B divides A, which are needed for the main theorem, which is in Section 4 along with some of its consequences. In particular $\det U_r$ is evaluated. Finally Section 5 shows that the operators developed are closely related to the Fourier transform on $L(A)$ (also known as the theory of Gaussian sums) and some consequences of this are obtained.

As general references for number theory we cite [1] and [4]. Only elementary aspects of representation theory are used, for which [2] is sufficient. Generally the letters $r, s, \ldots, z$ vary over R and ideal means integral ideal. Where the ideal A is understood it may be dropped from the notation, L for $L(A)$ and so on. If each of X, Y is a number in R or an ideal then (X, Y) denotes the ideal greatest common divisor of X and Y—in particular $(X, Y) = 1$ if and only if X, Y are relatively prime—and $X \mid Y$ signifies X divides Y. For P a prime ideal $v_P(X)$ denotes the multiplicity of P in X.

For $(r, A) = 1$, r^* is the inverse of $r \bmod A$, any element of R such that $rr^* \equiv 1 \bmod A$. In the symbol U_r it is taken for granted that $(r, A) = 1$. $\Gamma(A)$ is the group of characters of $G(A)$ and we refer to $\chi \in \Gamma(A)$ as a character χ (defined) $\bmod A$. Furthermore we always understand the character $\chi \bmod A$ also as the function χ' on R satisfying $\chi'(x) = \chi(x \bmod A)$ if $(x, A) = 1$ and $\chi'(x) = 0$ otherwise and χ' is again denoted simply χ. Thus $\chi \in L(A)$ and $\chi(xy) = \chi(x)\chi(y)$ for all x, y.

This last equation shows that $U_r\chi(x) = \chi(r)\chi(x)$ or $U_r\chi = \chi(r)\chi$. Let

$$L_\chi(A) = \{f \in L(A): U_r f = \chi(r) f \text{ for all } r\} \tag{2}$$

so that $\chi \in L_\chi$. Let $m(\chi)$ be the multiplicity of χ in U. By representation theory

$$L(A) = \oplus_\chi L_\chi(A) \qquad \text{and} \qquad m(\chi) = \dim L_\chi(A), \tag{3}$$

where the sum is over all $\chi \in \Gamma(A)$. The direct sum is also an orthogonal decomposition. Since $\chi \in L_\chi$ each $m(\chi)$ is $\geqslant 1$ and this suggests that perhaps the space L_χ may be constructed from χ. This indeed turns out to be true.

With respect to the basis $\{\delta_x\}$ it is seen that $U_r \delta_x = \delta_{r^*x}$ so that U is a permutation representation. Consequently

$$\det U_r = \pm 1 \qquad \text{and} \qquad \operatorname{trace} U_r = N(r - 1, A). \tag{4}$$

The latter holds since trace U_r is the number of δ_x's fixed by U_r, which is the

number of solutions $\bmod A$ to the congruence $r^*x \equiv x \bmod A$, which is $N(r-1, A)$. Finally we note that if $A = A_1A_2$, $(A_1, A_2) = 1$ then $L(A)$ may be identified with $L(A_1) \otimes L(A_2)$ by the isomorphism which maps $f_1 \otimes f_2 \in L(A_1) \otimes L(A_2)$ to the function $f \in L(A)$ given by $f(x) = f_1(x) f_2(x)$. This follows easily using the Chinese remainder theorem. In the same vein $G(A)$ may be identified with $G(A_1) \times G(A_2)$. With these identifications, if U^i is the representation of $G(A_i)$ on $L(A_i)$ for $i = 1, 2$, then

$$U \text{ is equivalent to } U^1 \otimes U^2. \tag{5}$$

The results of this paper are new even in the case that K is the rational field, R the ordinary ring of integers and the ideal A identified with a positive integer. But we have not stopped, after each theorem has been proved, to explicitly state the results for the rational case in particular, although this is of great interest.

2. Characters

Let A, M be ideals, α a character defined $\bmod M$ and suppose $M \mid A$. Define $\chi(x) = 0$ if $(x, A) \neq 1$ and $\chi(x) = \alpha(x)$ if $(x, A) = 1$. Then χ is a character $\bmod A$ said to be derived from α. χ is a primitive character $\bmod A$ if it cannot be derived from any $\alpha \bmod M$, where M is a proper divisor of A. It is known that given $\chi \bmod A$ there are uniquely determined an ideal $M \mid A$ and $\alpha \bmod M$ such that χ is derived from α and α is primitive. M is called the conductor of χ, denoted $M = M(\chi)$ and α is the primitive of χ. χ_0 denotes the trivial character $\bmod A$. χ_0 is the identity element of $\Gamma(A)$: $\chi_0(x) = 1$ if and only if $(x, A) = 1$, otherwise $\chi_0(x) = 0$. Clearly $M(\chi_0) = R$ and its primitive is α_0, the trivial character $\bmod R$, $\alpha_0(x) = 1$ for all x.

Later on we need some information about $\pi(A)$, the number of primitive characters defined $\bmod A$. To obtain this we recall that the apparatus of the theory of "arithmetic functions" defined on the natural numbers carries over in an obvious way to functions defined on the semigroup of integral ideals. Briefly, given two such functions λ, ν the Dirichlet convolution $*$ is defined by $\lambda * \nu(A) = \sum_{B \mid A} \lambda(B)\, \nu(A/B)$. $*$ is a commutative and associative operation. λ is called multiplicative if $\lambda(A) = \lambda(A_1)\, \lambda(A_2)$ whenever $A = A_1A_2$ with $(A_1, A_2) = 1$. A multiplicative function is determined by its values on prime powers and the convolution of multiplicative functions yields a multiplicative function. The Mobius function μ is defined by $\mu(A) = (-1)^k$ if A is the product of k distinct prime ideals and otherwise $\mu(A) = 0$. If $\mu(A) \neq 0$, A is called square free. Define ε by $\varepsilon(A) = 1$ for all A. Thus for any λ, $\lambda * \varepsilon(A) = \sum_{B \mid A} \lambda(B)$. $\mu * \varepsilon(A) = 0$ if $A \neq R$ and $\mu * \varepsilon(R) = 1$; $\mu * \varepsilon$ is the identity element for $*$. Mobius inversion is summarized by $\nu = \lambda * \varepsilon$ if

and only if $\lambda = \nu * \mu$. As examples, to be used, $\varphi(A)$, the order of $G(A)$, is a multiplicative function as is the norm N and it is well known that $N = \varphi * \varepsilon$. $\tau = \varepsilon * \varepsilon$ gives the number of divisors:

$$\tau(A) = \sum_{B|A} 1, \qquad \tau(P^k) = k+1, \qquad \tau(A) = \prod_{P|A} (v_P(A)+1).$$

In particular, $\tau(A)$ is odd if and only if A is a square ($A = B^2$ for some B) and otherwise $\tau(A)$ is even.

LEMMA 1. *Let $\pi(A)$ be the number of primitive characters defined* mod A. *π is multiplicative and*

$$\sum_{B|A} \pi(B)\,\tau(A/B) = NA, \qquad \sum_{\chi} \tau(A/M(\chi)) = NA$$

the sum being over all characters χ mod A.

Proof. $\Gamma(A)$ is isomorphic to $G(A)$ so there are $\varphi(A)$ characters mod A. Each character mod A is derived from a unique primitive character defined mod B for a unique divisor B of A and conversely each of the $\pi(B)$ primitive characters mod B gives rise to a character mod A. Thus $\varphi(A) = \sum_{B|A} \pi(B)$, $\varphi = \pi * \varepsilon$ and by Mobius inversion $\pi = \varphi * \mu$; thus π is multiplicative. Now $\pi * \tau = (\varphi * \mu) * (\varepsilon * \varepsilon) = \varphi * (\mu * \varepsilon) * \varepsilon = \varphi * \varepsilon = N$, which proves the first relation of the lemma. In the sum $\sum_\chi \tau(A/M(\chi))$ each of the $\pi(B)$ characters χ mod A whose conductor is B contributes $\tau(A/B)$ so their total contribution is $\pi(B)\,\tau(A/B)$. Thus the second relation is just a reformulation of the first.

The rest of this section is not needed for the main theorem but is necessary for the subsequent evaluation of $\det U_r$. We go into some detail since the statement in [4, p. 250, Proposition 6.6] about real primitive characters appears to be incorrect. Let $q(A)$ denote the number of real characters mod A; "q" for quadratic since χ is real if and only if $\chi(x) = \pm 1$ for $(x, A) = 1$ which is if and only if $\chi^2 = \chi_0$, i.e., χ has order 1 or 2 in $\Gamma(A)$. Let $c(A)$ be the number of real primitive characters mod A. Clearly a character is real if and only if its primitive is real so $q(A) = \sum_{B|A} c(B)$. Thus $q = c * \varepsilon$ and $c = q * \mu$. Since $\Gamma(A)$ is isomorphic to $G(A)$, $q(A)$ is also the number of solutions mod A to $x^2 \equiv 1 \bmod A$. It is well known that the number of solutions of this congruence is a multiplicative function of A; hence q and also c are multiplicative functions and it suffices to evaluate them on prime powers P^k. If $(2, P) = 1$ it is elementary that $x^2 \equiv 1 \bmod P^k$ has exactly 2 solutions for all $k \geqslant 1$. Thus $q(P^k) = 2$, $c(P^k) = q(P^k) - q(P^{k-1}) = 2 - 2 = 0$ for $k > 1$ and $c(P) = q(P) - q(R) = 2 - 1 = 1$. The unique real primitive character mod P is the (generalized) Legendre symbol: $(x/P) = 0$ if $P \mid x$ and otherwise $(x/P) = 1$ or -1 according as $x \bmod P$ is or is not a square in

$G(P)$. It follows by multiplicativity that if $(2, A) = 1$ then $c(A) = 0$ unless A is square-free in which case $c(A) = 1$. If A is square-free the unique real primitive character mod A is the (generalized) Jacobi symbol

$$\left(\frac{x}{A}\right) = \prod_{P|A} \left(\frac{x}{P}\right).$$

It remains to determine q and c for P^k when $P \mid 2$. Let $e = e(P/2)$ be the ramification index of P over 2. Making the substitution $x = 1 + y$ reduces $x^2 \equiv 1 \bmod P^k$ to $y(y+2) \equiv 0 \bmod P^k$. We let $v = v_P$; thus $v(2) = e$. Clearly a necessary condition for a solution is that $v(y) > 0$. Thus $q(P^k)$ is the number of $y \bmod P^k$ satisfying

$$v(y) > 0 \qquad \text{and} \qquad v(y) + v(y+2) \geqslant k. \tag{6}$$

We recall the basic properties of v: $v(rs) = v(r) + v(s)$ and $v(r+s) \geqslant \min(v(r), v(s))$ with equality holding whenever $v(r) \neq v(s)$.

Consider first the case $1 \leqslant k \leqslant 2e$. Assume y satisfies (6). If $v(y) < e$ then $v(y+2) = v(y)$ and so $2v(y) \geqslant k$, $v(y) \geqslant k/2$. If $v(y) \geqslant e$ then certainly $v(y) \geqslant k/2$ since $e \geqslant k/2$. Conversely any $y \in R$ satisfying $v(y) \geqslant k/2$ has $v(y+2) \geqslant \min(v(y), v(2)) \geqslant \min(k/2, e) = k/2$ so y satisfies (6). Thus $q(P^k)$ is the number of $y \bmod P^k$ with $v(y) \geqslant k/2$. If m is the smallest integer $\geqslant k/2$, $v(y) \geqslant k/2$ if and only if $y \equiv 0 \bmod P^m$ and so $q(P^k)$ is the index $|P^m : P^k| = NP^{k-m}$. Considering the cases k even, k odd it is seen that in either case $k - m = [k/2]$. Thus for $1 \leqslant k \leqslant 2e$, $q(P^k) = NP^{[k/2]}$ and $c(P^k) = NP^{[k/2]} - NP^{[(k-1)/2]}$, which reduces to 0 if k is odd and to $NP^{k/2} - NP^{k/2-1}$ if k is even.

Now consider $k \geqslant 2e + 1$. If y satisfies (6) then at least one of $v(y)$, $v(y+2)$ must be greater than e. Assume first $v(y) > e$; hence $v(y+2) = e$ so (6) implies $v(y) \geqslant k - e$. Conversely any y with $v(y) \geqslant k - e > e$ has then $v(y+2) = e$ and (6) is satisfied. Thus the solutions of (6) with $v(y) > e$ are just all y satisfying $y \equiv 0 \bmod P^{k-e}$ and mod P^k there are $|P^{k-e} : P^k| = NP^e$ such solutions. Finally we have to count the number of $y \bmod P^k$ satisfying (6) with $v(y) \leqslant e$; in this case then it is necessary that $v(y+2) > e$. Setting $z = y + 2$ we have to count the number of $z \bmod P^k$ satisfying $v(z) > e$, $v(z) + v(z-2) \geqslant k$. Arguing as was just done, with z now in place of y, it is seen that the number of such z is also NP^e. The totality of $2(NP^e)$ solutions obtained are all different mod P^k. For if y is any solution in the former set and y' any in the latter then $v(y) \geqslant k - e$, $v(y'+2) \geqslant k - e$; hence $y' \equiv y \bmod P^k$ implies $y' \equiv y \equiv 0 \bmod P^{k-e}$ and so $2 \equiv y' + 2 \equiv 0 \bmod P^{k-e}$, which is absurd since $k - e > e$. Thus for all $k \geqslant 2e + 1$, $q(P^k) = 2(NP^e)$; hence $c(P^{2e+1}) = q(P^{2e+1}) - q(P^{2e}) = 2(NP^e) - NP^e = NP^e$, while for $k > 2e + 1$, $c(P^k) = q(P^k) - q(P^{k-1}) = 0$. We summarize these results.

THEOREM 1. *Let P be a prime ideal, $P \mid 2$ and $e = e(P/2)$. Let k be a positive integer. $q(P^k)$, the number of real characters* mod P^k, *is*

$$\begin{aligned} q(P^k) &= NP^{[k/2]}, && \text{if } 1 \leqslant k \leqslant 2e \\ &= 2(NP^e), && \text{if } k \geqslant 2e+1. \end{aligned}$$

$c(P^k)$, the number of real primitive characters mod P^k, *is*

$$\begin{aligned} c(P^k) &= 0, && \text{if } k \text{ is odd and } 1 \leqslant k < 2e \\ &= NP^{k/2} - NP^{k/2-1}, && \text{if } k \text{ is even and } 1 < k \leqslant 2e \\ &= NP^e, && \text{if } k = 2e+1 \\ &= 0, && \text{if } k > 2e+1. \end{aligned}$$

In any finite abelian group H the p-rank (p a prime) of H is the number of cyclic factors of order a power of p when H is expressed as a product of cyclic groups of prime power order. In particular take $p = 2$ and let ρ be the 2-rank. Then ρ is also the 2-rank of the subgroup H' consisting of all $h \in H$ satisfying $h^2 = 1$ and the order of H' is 2^ρ. For an ideal A let $\rho(A)$ be the 2-rank of $\Gamma(A)$. Thus $2^{\rho(A)}$ is the number of $\chi \in \Gamma(A)$ with $\chi^2 = \chi_0$, i.e., $2^{\rho(A)} = q(A)$. Since q is multiplicative ρ is additive. For $P \mid 2$ let $f = f(P/2)$ be the degree of P over 2; $NP = 2^f$. Taking this into account along with $2^{\rho(P^k)} = q(P^k)$ and the values of $q(P^k)$ given in the above theorem we have:

COROLLARY. *If $P \mid 2$, $f = f(P/2)$ then $\rho(P^k)$, the 2-rank of $\Gamma(P^k)$, is also the 2-rank of the subgroup of all real characters* mod P^k *and is given by*

$$\begin{aligned} \rho(P^k) &= f[k/2], && \text{if } 1 \leqslant k \leqslant 2e \\ &= fe + 1, && \text{if } k \geqslant 2e+1. \end{aligned}$$

After this was written the article [3] was observed in which the p-rank of $G(P^k)$ is obtained, from which the above can be deduced with $p = 2$. However, the method we have used, though not as general, is simpler for our particular purposes.

3. THE OPERATORS I, J

Although ideals need not be principal, our concern is essentially with ideals B mod A of the ring R mod A, $B \mid A$, and these are principal. To this end we need a choice function s that selects, for each such B, an element $s(B) \in B$ which generates the ideal B mod A.

Let $P_1,\ldots,P_m$ be a given finite number of prime ideals and let T be the semigroup of ideals generated by them. Thus $B \in T$ if and only if $v_P(B) = 0$ for all $P \neq P_i$, $1 \leqslant i \leqslant m$. For each i choose an element $s_i \in P_i$ such that $v_{P_i}(s_i) = 1$ and $v_{P_j}(s_i) = 0$ for $1 \leqslant i, j \leqslant m$, $i \neq j$. The s_i are not unique but make some fixed choice. For $B \in T$ let $k_i = v_{P_i}(B)$ and

$$s(B) = \prod_{i=1}^{m} s_i^{k_i}.$$

Clearly $s(B) \in B$ and $s(R) = 1$.

The following lemma will be used repeatedly; the proof is straightforward hence omitted.

LEMMA 2. *If $A \in T$ and $B \mid A$ then $B \in T$. Suppose $A \in T$, $A = BB'$. Then*

(a) $s(A) = s(B)\, s(B')$.

(b) $(s(B), A) = B$ *and* $(s(B)/B, A) = 1$.

(c) *As u, v range over sets of representatives of $R \bmod B$, $R \bmod B'$, respectively, $s(B)v + u$ ranges over a set of representatives of $R \bmod A$.*

(d) *Given $x \in B'$ there exists $y \in R$ such that $x \equiv s(B')y \bmod A$. If also $x \equiv s(B')z \bmod A$ then $z \equiv y \bmod B$.*

In the rest of this section all ideals are understood to be in T and a choice function s is fixed. Let $B \mid A$, $B' = A/B$. For $f \in L(B)$ define

$$I_A^B f(x) = \left(\frac{NB}{NA}\right)^{1/4} f(x), \tag{7}$$

$$\begin{aligned} J_A^B f(x) &= 0, && \text{if } x \not\equiv 0 \bmod B' \\ &= \left(\frac{NB}{NA}\right)^{-1/4} f(y), && \text{if } x \equiv 0 \bmod B' \\ & && \text{and } x \equiv s(B')y \bmod A. \end{aligned} \tag{8}$$

It is clear that I_A^B is a linear operator from $L(B)$ to $L(A)$. It is not obvious that $J_A^B f$ is well defined, but note that if also $x \equiv s(B')z \bmod A$ then $z \equiv y \bmod B$; hence $f(z) = f(y)$ since $f \in L(B)$ so $J_A^B f$ is well defined. Observe also that if $x \in R$ satisfies $x \equiv s(B')y \bmod A$ for some y then indeed $x \equiv 0 \bmod B'$ so the definition of $g = J_A^B f$ may be formulated as

$$g(x) = \left(\frac{NB}{NA}\right)^{-1/4} f(y)$$

if $x \equiv s(B')y \bmod A$ for some y and otherwise $g(x) = 0$. If $u \equiv x \bmod A$ then

$x \equiv s(B')y \bmod A$ if and only if $u \equiv s(B')y \bmod A$ so $J_A^B f(x) = J_A^B f(u)$. This shows $J_A^B f \in L(A)$ and J_A^B is a linear operator from $L(B)$ to $L(A)$. We now present some important properties of these operators.

THEOREM 2. (a) *Isometry: for* $f, g \in L(B)$

$$(I_A^B f, I_A^B g)_A = (f, g)_B \qquad \text{and} \qquad (J_A^B f, J_A^B g)_A = (f, g)_B.$$

(b) *Transitivity: if* $C \mid B$ *and* $B \mid A$ *then*

$$I_A^B I_B^C = I_A^C,\ J_A^B J_B^C = J_A^C \text{ and } I_A^A = J_A^A = \text{identity map on } L(A).$$

(c) *Quasi-commutativity: if* $C \mid B$, $B \mid A$ *and* $D = AC/B$ *then*

$$J_A^B I_B^C = I_A^D J_D^C.$$

(d) *For* $(r, A) = 1$ *let* U_r *denote the operator associated to* r *on* $L(B)$ *as well as on* $L(A)$. *Then*

$$U_r I_A^B = I_A^B U_r \qquad \text{and} \qquad U_r J_A^B = J_A^B U_r.$$

Proof. We keep throughout the proof the notation $A = BB'$, $B = CC'$.

(a) Choose a set of representatives of $R \bmod A$ as $x = s(B)v + u$, $u \bmod B$, $v \bmod B'$. Then $x \equiv u \bmod B$, so for $f \in L(B)$, $f(x) = f(u)$ for each of the NB' v's. Thus

$$(I_A^B f, I_A^B g)_A = \frac{1}{\sqrt{NA}} \left(\frac{NB}{NA}\right)^{1/2} \sum_{\substack{u \bmod B \\ v \bmod B'}} f(s(B)v + u)\, \overline{g(s(B)v + u)}$$

$$= \frac{1}{\sqrt{NA}} \left(\frac{NB}{NA}\right)^{1/2} NB' \sum_{u \bmod B} f(u)\, \overline{g(u)} = (f, g)_B.$$

To show J_A^B an isometry choose the representatives x of $R \bmod A$ as $x = s(B')u + v$, $u \bmod B$, $v \bmod B'$ and so that $v = 0$ is the representative of $0 \bmod B'$. Then for $f \in L(B)$, $J_A^B f(x) = 0$ unless $x \equiv 0 \bmod B'$, which is if and only if $v = 0$, and then $J_A^B f(x) = (NB/NA)^{-1/4} f(u)$. Thus $(J_A^B f, J_A^B g)_A = (1/\sqrt{NA})(NB/NA)^{-1/2} \sum_{u \bmod B} f(u)\, \overline{g(u)} = (f, g)_B$.

(b) We only prove the J assertion, the rest is obvious. Let $f \in L(C)$, $g = J_B^C f$ and $h = J_A^B g$. For any x, $h(x) = (NB/NA)^{-1/4} g(y)$ if, for some y,

$$x \equiv s(B')y \bmod A \tag{9}$$

otherwise $h(x) = 0$. But $g(y) = 0$ unless, for some z,

$$y \equiv s(C')z \bmod B, \tag{10}$$

in which case $g(y) = (NC/NB)^{-1/4} f(z)$. Equation (10) may be expressed as $y = s(C')z + w$, for some $w \in B$, and inserting this into (9) yields $x \equiv s(B')\,s(C')z + s(B')w \bmod A$. But $s(B')\,s(C') = s(B'C')$ and $s(B')w \equiv 0 \bmod B'B = A$; hence $x \equiv s(B'C')z \bmod A$. Thus $h(x) = 0$ unless $x \equiv s(B'C')z \bmod A$, in which case $h(x) = (NC/NA)^{-1/4} f(z)$, which says $h = J_A^C f$, since $A/C = B'C'$.

(c) $D = AC/B = B'C$ shows that D is integral and $C \mid D$, while $A/D = B/C = C'$ shows $D \mid A$ and $A = DC'$. Let $f \in L(C)$, $g = J_A^B I_B^C f$ and $h = I_A^D J_D^C f$. $g(x) = 0$ unless $x \equiv s(B')y \bmod A$, for some y, in which case $g(x) = (NB/NA)^{-1/4}(NC/NB)^{1/4} f(y)$. $h(x) = 0$ unless $x \equiv s(B')z \bmod D$, for some z (since $D/C = B'$), in which case $h(x) = (ND/NA)^{1/4}$ $(NC/ND)^{-1/4} f(z)$. The norm constants have the same value for $g(x)$, $h(x)$ and, since $D \mid A$, the congruence $\bmod A$ may be read $\bmod D$ to yield $s(B')z \equiv x \equiv s(B')y \bmod D$. Thus $z \equiv y \bmod D/B' = C$ and $f(y) = f(z)$ since $f \in L(C)$. Thus $g = h$ as required.

(d) The I assertion is immediate from the definitions. For $f \in L(B)$ let $g = J_A^B U_r f$ and $h = U_r J_A^B f$. $g(x) = 0$ unless $x \equiv 0 \bmod B'$ in which case $g(x) = (NB/NA)^{-1/4} f(ry)$, where $x \equiv s(B')y \bmod A$. $h(x) = 0$ unless $rx \equiv 0 \bmod B'$, which is if and only if $x \equiv 0 \bmod B'$, in which case $h(x) = (NB/NA)^{-1/4} f(z)$, where $rx \equiv s(B')z \bmod A$. But $x \equiv s(B')y \bmod A$ gives $rx \equiv s(B')ry \bmod A$; hence $z \equiv ry \bmod B$, in which the case $f(z) = f(ry)$ since $f \in L(B)$. Thus $g = h$. This completes the proof of the theorem.

4. The Main Theorem

Fix the ideal A, take T to be the semigroup generated by the prime divisors of A and s an appropriate choice function. In particular, the operators I_B^C, J_B^C are now defined whenever C, B are divisors of A and $C \mid B$.

Theorem 3. *Let χ be a character defined* $\bmod A$ *with conductor $M = M(\chi)$ and primitive α defined* $\bmod M$. *For each divisor D of A/M let $W_D = I_A^{MD} J_{MD}^M$. W_D is an isometry from $L(M)$ to $L(A)$. The set of functions $\{W_D \alpha\}$, D ranging over the divisors of A/M, is linearly independent and is a basis for the subspace $L_\chi(A)$. $m(\chi)$, the multiplicity of χ in U, is $\tau(A/M(\chi))$, the number of divisors of $A/M(\chi)$.*

Proof. By Theorem 2, W_D is a composition of isometries; hence it is also an isometry. Suppose now there are constants c_D, D ranging over the divisors of A/M, such that $\Sigma_D c_D W_D \alpha = 0$:

$$\text{for all } x, \qquad \Sigma_D c_D W_D \alpha(x) = 0. \tag{11}$$

Now $W_D\alpha(x) = 0$ unless $x \equiv 0 \bmod D$, in which case $W_D\alpha(x) = h_D\alpha(y)$, where $x \equiv s(D)y \bmod MD$ and h_D is a non-zero constant,

$$h_D = \left(\frac{N(MD)}{NA}\right)^{1/4}\left(\frac{NM}{N(MD)}\right)^{-1/4}.$$

In particular, with $x = 1$ in (11) the only D for which $W_D\alpha(1) \neq 0$ is when $1 \equiv 0 \bmod D$, i.e., $D = R$, in which case, since $s(R) = 1$, we may take $y = 1$ also. Thus (11) reduces to $c_R h_R \alpha(1) = 0$. But $h_R \neq 0$, $\alpha(1) = 1 \neq 0$; hence $c_R = 0$. We proceed by induction on $\Omega(D)$, the total number, counting multiplicities, of prime factors of D: $\Omega(D) = \Sigma_P v_P(D)$. The only ideal D with $\Omega(D) = 0$ is $D = R$ and we have just shown $c_R = 0$. Assume now n is a positive integer and that $c_D = 0$ for all D with $\Omega(D) < n$. Let D_1 have $\Omega(D_1) = n$. Equation (11) now becomes

$$\text{for all } x, \qquad c_{D_1} W_{D_1}\alpha(x) + \Sigma'_D c_D W_D\alpha(x) = 0, \tag{12}$$

where Σ'_D indicates the sum over all divisors D of A/M having $\Omega(D) \geqslant n$ and $D \neq D_1$. In (12) take $x = s(D_1)$. Then $W_{D_1}\alpha(x) = h_{D_1}\alpha(1) \neq 0$. For the D in Σ' we claim $W_D\alpha(x) = 0$. Indeed, otherwise $x = s(D_1) \equiv 0 \bmod D$ and since D, D_1 are both divisors of A this would imply $D \mid (s(D_1), A) = D_1$, which is impossible for $\Omega(D) \geqslant \Omega(D_1)$ and $D \neq D_1$. Thus (12) reduces to $c_{D_1} h_{D_1}\alpha(1) = 0$, yielding $c_{D_1} = 0$. This proof by induction shows that all $c_D = 0$; hence the set $\{W_D\alpha\}$ is linearly independent in $L(A)$. We remark that so far no use has been made of the fact that α is a character, all that was used was $\alpha \in L(M)$ and $\alpha(1) \neq 0$. But since α is the primitive of χ it follows that for $(r, A) = 1$, $\chi(r) = \alpha(r)$ and, denoting by U_r, for $B \mid A$, the operator on $L(B)$ associated with r, as well as on $L(A)$, $U_r\alpha = \alpha(r)\alpha$ just as $U_r\chi = \chi(r)\chi$. Thus, by a double application of Theorem 2(d), $U_r(W_D\alpha) = W_D(U_r\alpha) = W_D(\alpha(r)\alpha) = \alpha(r)\, W_D\alpha = \chi(r)\, W_D\alpha$, so each $W_D\alpha \in L_\chi(A)$. Thus $\dim L_\chi(A) \geqslant \tau(A/M(\chi))$, since this is the number of functions in the linearly independent set $\{W_D\alpha\}$ contained in $L_\chi(A)$. Taking this into account with (3) and Lemma 1, we have

$$NA = \dim L(A) = \Sigma_\chi \dim L_\chi(A) \geqslant \Sigma_\chi \tau\left(\frac{A}{M(\chi)}\right) = NA.$$

Since all the numbers involved are non-negative this forces $\dim L_\chi(A) = \tau(A/M(\chi))$, which completes the proof of the theorem upon recalling $m(\chi) = \dim L_\chi(A)$.

For each χ use the basis $\{W_D\alpha\}$ in L_χ. Stringing these together one obtains a basis for $L = \bigoplus L_\chi$. With respect to this basis U_r is represented by a diagonal matrix in which, for each χ, $\chi(r)$ occurs $m(\chi)$ times along the diagonal.

Thus

$$\text{trace } U_r = \sum_{\chi}{}' m(\chi)\,\chi(r) \qquad \text{and} \qquad \det U_r = \prod_{\chi}{}' \chi(r)^{m(\chi)}. \tag{13}$$

Comparing this with the trace given in (4) there results

$$\sum_{\chi}{}' \tau\left(\frac{A}{M(\chi)}\right)\chi(r) = N(r-1, A). \tag{14}$$

This may be inverted by a standard method. Fix a character Ψ and multiply both sides by $\Psi(r)$. Sum over r ranging over a set of representatives of $G(A)$ and use the character relation $\sum_r \chi(r)\,\Psi(r) = 0$ unless $\chi = \bar{\Psi}$, in which case it is $\varphi(A)$, the order of $G(A)$. Finally, replacing again Ψ by χ and noting $M(\bar{\chi}) = M(\chi)$ there results: for any character $\chi \bmod A$

$$\sum_{r}{}' N(r-1, A)\,\chi(r) = \varphi(A)\,\tau\left(\frac{A}{M(\chi)}\right). \tag{15}$$

Here $\sum_r'$ is a reminder that the sum is over a set of representatives of $R \bmod A$ having $(r, A) = 1$. Specializing to $\chi = \chi_0$, $M(\chi_0) = R$, one has

$$\sum_{r}{}' N(r-1, A) = \varphi(A)\,\tau(A). \tag{16}$$

Now χ is a primitive character $\bmod A$ if and only if $M(\chi) = A$, which is if and only if $\tau(A/M(\chi)) = 1$. Thus we have the following criterion for a character to be primitive:

χ is a primitive character $\bmod A$ if and only if

$$\sum_{r}{}' N(r-1, A)\,\chi(r) = \varphi(A). \tag{17}$$

Now consider $\det U_r$. Since $\det U_{rs} = \det U_r \det U_s$, $r \to \det U_r$ is a character $\bmod A$ which we denote $\det U$. Equation (13) may be expressed simply as

$$\det U = \prod_{\chi}{}' \chi^{m(\chi)}. \tag{18}$$

If χ is not a real character then $\chi \neq \bar{\chi}$, $m(\chi) = m(\bar{\chi})$ and χ, $\bar{\chi}$ contribute to the above product $(\chi\bar{\chi})^{m(\chi)} = \chi_0$; hence may be dropped. If χ is real, $\chi^2 = \chi_0$, so $\chi^{m(\chi)} = \chi_0$ if $m(\chi)$ is even and $\chi^{m(\chi)} = \chi$ if χ is odd. Thus $\det U$ is the product of all real χ for which $m(\chi)$ is odd. But $m(\chi) = \tau(A/M(\chi))$ is odd if and only if $A/M(\chi)$ is a square. Call χ–for lack of a better name—special if χ is real and $A/M(\chi)$ is a square. Thus (18) reduces to

$$\det U = \prod_{\chi \text{ special}}{}' \chi. \tag{19}$$

Of course if there are no special characters mod A the empty product is χ_0. If $(A, 2) = 1$ it is easy to enumerate the special characters. In fact, if χ is special with primitive $\alpha \bmod M = M(\chi)$ then α is a real primitive character mod M. By the discussion in Section 2, M must be square-free and $\alpha(x) = (x/M)$, the Jacobi symbol. But M square-free and also $A = MB^2$, for some B, implies that M is the square-free part of A. Hence M, α and also χ are unique. This proves the first part of the following theorem evaluating $\det U$.

THEOREM 4. (a) *If* $(A, 2) = 1$, $\det U_r = (r/M)$, *where* M *is the square-free part of* A. *In particular,* $\det U_r = 1$ *for all* r *if and only if* A *is a square.*

(b) *If* $(A, 2) \neq 1$ *then* $\det U_r = 1$ *for all* r *except if* $A = A_1 P^k$ *with* $(A_1, 2) = 1$ *and* $P \mid 2$, $k \geqslant 1$. *In this case let* $e = e(P/2)$, $f = f(P/2)$. *Then again* $\det U_r = 1$ *for all* r *except if*

$$f = 1,\ e = 1,\ k \geqslant 2 \tag{20}$$

or

$$f = 1,\ e > 1,\ k = 2. \tag{21}$$

In these cases $\det U_r = 1$ *if* $r \equiv 1 \bmod P^2$ *and* $\det U_r = -1$ if $r \not\equiv 1 \bmod P^2$.

Proof. Assume $(A, 2) \neq 1$. It is not so easy now to enumerate the special characters mod A. Instead we argue as follows. Write $A = A_1 A_2$, where $(A_1, 2) = 1$ and A_2 involves only primes dividing 2: $A_1 = \prod_{P \nmid 2} P^{v_P(A)}$ and $A_2 = \prod_{P \mid 2} P^{v_P(A)}$. By (5), $\det U_r = \det(U_r^1 \otimes U_r^2)$. The determinant of the tensor product is then easily seen, since we have diagonalized our operators, to be $(\det U_r^1)^{NA_2} (\det U_r^2)^{NA_1}$. But each $\det = \pm 1$, NA_2 is even and NA_1 is odd. Hence $\det U_r = \det U_r^2$. Now suppose there are at least two primes P_1, P_2 such that $P_1 \mid 2$, $P_2 \mid 2$ and $P_1 P_2 \mid A$. Then we may write $A_2 = A_3 A_4$ where $A_3 = P_1^{v_{P_1}(A)}$ and $A_4 = A_2 / A_3$. Thus $(A_3, A_4) = 1$ so again by (5), with an obvious notation,

$$\det U_r^2 = \det(U_r^3 \otimes U_r^4) = (\det U_r^3)^{NA_4} (\det U_r^4)^{NA_3} = 1$$

since NA_3, NA_4 are both even. Hence $\det U_r = 1$ for all r in this case and we are reduced to considering the case $A_2 = P^k$ with $P \mid 2$, $k \geqslant 1$, $A = A_1 P^k$, $\det U_r = \det U_r^2$, where U_r^2 is the operator associated to r on $L(P^k)$. To indicate the independence on k we write $d_k = \det U^2$; thus $\det U_r = d_k(r)$. We can now dispense with A and concentrate on d_k, the determinant of the representation of $G(P^k)$ on $L(P^k)$. By (19), d_k is the product of all special characters defined mod P^k. The conductor of a special χ has $P^k / M(\chi)$ a

square; hence $M(\chi) = P^h$ with $0 \leqslant h \leqslant k$ and $h \equiv k \bmod 2$. Thus (19) becomes

$$d_k = \prod_{\substack{0 \leqslant h \leqslant k \\ h \equiv k \bmod 2}} \left(\prod_{\substack{\chi \text{ real} \\ M(\chi) = P^h}} \chi \right). \tag{22}$$

By Theorem 1 there are no real primitive characters mod P and the only real primitive character mod $P^0 = R$ is the trivial character. Thus $d_1 = \chi_0$, $\det U_r = 1$ for all r if $k = 1$. Assume from now on $k \geqslant 2$; in (22) the range of h may be taken as $2 \leqslant h \leqslant k$. Observe that a character $\chi \bmod P^k$ and its primitive $\alpha \bmod P^h$ are identical as functions on R, for $\chi(x) = \alpha(x)$ if $(x, P^k) = 1$, i.e., if $(x, P) = 1$ and otherwise $\chi(x) = \alpha(x) = 0$. Thus we now do not distinguish notationally between them. Let X_h be the group of real characters defined mod P^h. Then X_{h-1} may be identified as a subgroup of X_h and X_{h-1} consists precisely of those real characters that are not primitive mod P^h. Thus in (22) the inner product may be written

$$\prod_{\substack{\chi \in X_h \\ \chi \notin X_{h-1}}} \chi = \left(\prod_{\chi \in X_h} \chi \right) \cdot \left(\prod_{\chi \in X_{h-1}} \chi \right),$$

since all these characters have order 2 (or 1). Let $\varepsilon_h = \prod_{\chi \in X_h} \chi$ so (22) becomes

$$d_k = \prod_{\substack{2 \leqslant h \leqslant k \\ h \equiv k \bmod 2}} (\varepsilon_h \varepsilon_{h-1}) = \varepsilon_k \varepsilon_{k-1} \cdots \varepsilon_2 \tag{23}$$

since $\varepsilon_1 = \chi_0$. To evaluate ε_h we use the following remark: Let G be a finite abelian group and $z = \prod_{x \in G} x$, the product of all the elements of G. Then z is the identity of G except if G has a unique element of order 2 in which case z is that element. A group has a unique element of order 2 if and only if its 2-rank is 1. Proof of this is not difficult and left to the reader. Thus $\varepsilon_h = \chi_0$ except if the 2-rank of X_h is 1. The 2-rank of X_h, $\rho(P^h)$ is given in the corollary to Theorem 1. As usual, with $e = e(P/2)$, $f = f(P/2)$, we see that $\rho(P^h)$ is 1 if and only if $f = 1$, $h = 2$ or $f = 1$, $h = 3$ and $e > 1$. Thus each $\varepsilon_h = \chi_0$ if $f > 1$ and so $\det U_r = 1$ for all r in this case. Assume now $f = 1$. Since $\varepsilon_h = \chi_0$ certainly for $h \geqslant 4$, (23) reduces to

$$d_2 = \varepsilon_2 \qquad \text{and} \qquad d_k = \varepsilon_3 \varepsilon_2 \qquad \text{for} \quad k \geqslant 3. \tag{24}$$

What is ε_2? Since $f = 1$, a set of representatives of $R \bmod P^2$ is given by $0, 1, u, 1 + u$ where $u \in R$ is any element with $v_P(u) = 1$. $G(P^2)$ is the cyclic group of order 2 consisting of $1 \bmod P^2$ and $1 + u \bmod P^2$. Clearly the unique non-trivial real character $\bmod P^2$ is given by $\psi(x) = 1$, if

$x \equiv 1 \bmod P^2$ and $\psi(x) = -1$ if $x \not\equiv 1 \bmod P^2$ and $(x, P) = 1$. ψ is primitive $\bmod P^2$. Thus $\varepsilon_2 = \psi$. If $e = 1$ then $\rho(P^3) \neq 1$; hence $\varepsilon_3 = \chi_0$. Thus (24) shows that $d_k = \varepsilon_2 = \psi$ for all $k \geqslant 2$ in this case, which is (20) above. Finally, suppose $e > 1$. Then $\rho(P^3) = 1$ and ε_3 is the unique element of order 2 in X_3. But ψ, considered $\bmod P^3$, is an element of order 2 in X_3; hence $\varepsilon_3 = \psi$. Thus for $k \geqslant 3$, (24) shows $d_k = \varepsilon_3 \varepsilon_2 = \psi^2 = \chi_0$. The only remaining case is (21), where we have seen $d_2 = \varepsilon_2 = \psi$. This completes the proof of the theorem.

5. The Fourier Transform

To define the Fourier transform as a unitary operator on $L(A)$ we first must establish an identification of the additive group $R \bmod A$ with its dual group. Furthermore we wish to do this "uniformly" for all $R \bmod B$, where $B \mid A$. Fix the ideal A. Let Δ be the different of K/Q and $A^* = A^{-1}\Delta^{-1}$ the complementary fractional ideal relative to the trace of K/Q. Thus $\operatorname{tr}(\xi x) \in \mathbb{Z}$ for all $x \in A$ if and only if $\xi \in A^*$. Choose $a^* \in A^*$ so that (as a fractional ideal) $a^* = A^* X$, where X is an integral ideal and $(X, A) = 1$. Define the function Φ on $R \times R$ by $\Phi(x, y) = e^{2\pi i \operatorname{tr}(a^* xy)}$. $|\Phi(x, y)| = 1$, $\Phi(x, y)$ depends only on $x \bmod A$, $y \bmod A$, is symmetric, $\Phi(x_1 + x_2, y) = \Phi(x_1, y)\,\Phi(x_2, y)$ and $\Phi(x, -y) = \overline{\Phi(x, y)}$. Thus for fixed y, $x \bmod A \to \Phi(x, y)$ is a character of the additive group $R \bmod A$ and this character is trivial if and only if $y \equiv 0 \bmod A$. Thus Φ induces a proper pairing on $R \bmod A$ with itself giving the desired identification of $R \bmod A$ with its dual. As usual, we denote this induced map also as Φ. Now let $B \mid A$, $A = BB'$. The number $b^* = s(B')\,a^*$ is (as a fractional ideal) $b^* = s(B')A^{-1}\Delta^{-1}X = (s(B')/B')(X/(B\Delta))$ and $Y = s(B')/B'$ is integral and prime to A; hence B. Thus $b^* = B^* YX$ with YX integral and $(YX, B) = 1$. As was just done with A it follows that defining $\Phi_B(x, y) = e^{2\pi i \operatorname{tr}(b^* xy)}$ induces an identification of $R \bmod B$ with its dual. Our notation now is: for each $B \mid A$, $\Phi_B(x, y) = \Phi(s(B')x, y)$, where $B' = A/B$. In particular, $\Phi_A = \Phi$.

For each $B \mid A$ we define the Fourier transform $F_B : L(B) \to L(B)$ as follows: for $f \in L(B)$

$$F_B f(x) = \frac{1}{\sqrt{NB}} \sum_{y \bmod B} f(y)\,\Phi_B(y, -x). \tag{25}$$

The basic properties follow by the general theory but here are easily verified directly. We state them in terms of $F = F_A$ on $L(A)$ but they hold of course for each F_B on $L(B)$:

$$F \text{ is a unitary operator on } L(A),\ F^2 = U_{-1},\ F^4 = \text{identity} \tag{26}$$

and, for $(r, A) = 1$,

$$U_r F = F U_{r^*}. \tag{27}$$

Actually (27) does not follow just from abelian group theory since it uses the ring structure on $R \bmod A$ and the fact that Φ satisfies $\Phi(xz, y) = \Phi(x, zy)$ for all x, y, z.

Our definition of F involved the choice of $a^* \in A^*$. If some other $a^{**} \in A^*$ were chosen, with the same required properties, then it is not hard to see that the new F, associated with the new Φ, would differ from the original one only by some U_r. Thus the finite group of unitary operators generated by the U_r's and F is "intrinsic" in some sense.

THEOREM 5. *If $B \mid A$, then*

$$F_A I_A^B = J_A^B F_B \qquad \text{and} \qquad F_A J_A^B = I_A^B F_B.$$

Proof. For $f \in L(B)$ let $g = F_A I_A^B f$:

$$g(x) = \frac{1}{\sqrt{NA}} \sum_{y \bmod A} \left(\frac{NB}{NA}\right)^{1/4} f(y)\, \Phi_A(y, -x).$$

Choose the representatives $y \bmod A$ as $y = s(B)v + u$, $v \bmod B' = A/B$ and $u \bmod B$. Then $f(y) = f(u)$, $\Phi_A(y, -x) = \Phi_A(s(B)v, -x)\, \Phi_A(u, -x) = \Phi_{B'}(v, -x)\, \Phi_A(u, -x)$. Hence

$$g(x) = \frac{1}{\sqrt{NA}} \left(\frac{NB}{NA}\right)^{1/4} \sum_{u \bmod B} f(u)\, \Phi_A(u, -x) \sum_{v \bmod B'} \Phi_{B'}(v, -x).$$

By the character relations for an abelian group the inner sum over $v \bmod B'$ is 0, unless $x \equiv 0 \bmod B'$, in which case the sum is NB'. For $x \equiv 0 \bmod B'$ write $x \equiv s(B')z \bmod A$, for some z, $\Phi_A(u, -x) = \Phi_A(u, -s(B')z) = \Phi_A(s(B')u, -z) = \Phi_B(u, -z)$. Thus $g(x) = 0$ unless $x \equiv s(B')z \bmod A$, for some z, in which case

$$g(x) = \frac{1}{\sqrt{NA}} \left(\frac{NB}{NA}\right)^{1/4} \cdot NB' \sum_{u \bmod B} f(u)\, \Phi_B(u, -z) = \left(\frac{NB}{NA}\right)^{-1/4} F_B f(z);$$

thus $g = J_A^B F_B f$. We remark that it was precisely this calculation that led to the discovery of the operator J_A^B. The second relation in the theorem may be proved similarly but it is simpler to observe that multiplying the proved relation $F_A I_A^B = J_A^B F_B$ on the left by F_A and on the right by F_B gives $F_A^2 I_A^B F_B = F_A J_A^B F_A^2$. But $F_A^2 = U_{-1}$ on $L(A)$, $F_B^2 = U_{-1}$ on $L(B)$ and since U_{-1} commutes with all these operators the relation $I_A^B F_B = F_A J_A^B$ follows.

We also note that with the Fourier transform available some parts of

Theorem 2 can be obtained in a simpler way by making use of the relation just proved in the form $J_A^B = F_A I_A^B F_B^{-1}$.

With respect to the basis $\{\delta_x\}_{x \bmod A}$ of $L(A)$ one obtains $F\delta_x = \sum_{y \bmod A} (\Phi(x,-y)/\sqrt{NA})\,\delta_y$ (dropping the subscript A from F and Φ). The matrix of F with respect to this basis is thus

$$\left(\frac{\overline{\Phi(x,y)}}{\sqrt{NA}}\right)_{x,y \bmod A},$$

assuming some fixed ordering of the representatives $\bmod A$. In particular then

$$\operatorname{trace} F = \frac{1}{\sqrt{NA}} \sum_{x \bmod A} e^{-2\pi i \operatorname{tr}(a^* x^2)}. \tag{28}$$

If $f \in L(A)$ is any completely multiplicative function, $f(x_1 x_2) = f(x_1) f(x_2)$ for all $x_1, x_2 \in R$, then for $(r, A) = 1$,

$$Ff(rx) = \frac{1}{\sqrt{NA}} \sum_{y \bmod A} f(y)\,\Phi(y, -rx).$$

Making the change of variable $y \equiv r^* z \bmod A$, a little calculation shows

$$Ff(rx) = \frac{f(r^*)}{\sqrt{NA}} \sum_{\bmod A} f(z)\,\Phi(z,-x) = f(r^*)(Ff(x)).$$

In particular, taking f to be a character $\chi \bmod A$, $\chi(r^*) = \bar{\chi}(r)$

$$F\chi(rx) = \overline{\chi(r)}(F\chi(x)), \qquad F\chi(r) = \bar{\chi}(r)(F\chi(1)) \tag{29}$$

the second resulting from the first with $x = 1$. Suppose now χ is a primitive character $\bmod A$ and $(x, A) \neq 1$, $(x, A) = B$, say. Then $B' = A/B$ is a proper divisor of A and since χ is primitive $\bmod A$ there exists some r such that $(r, A) = 1$, $r \equiv 1 \bmod B'$ and $\chi(r) \neq 1$. Also $x(r-1) \equiv 0 \bmod BB' = A$, so $rx \equiv x \bmod A$. Thus $F\chi(x) = F\chi(rx) = \bar{\chi}(r)(F\chi(x))$. Since $\overline{\chi(r)} \neq 1$ this forces $F\chi(x) = 0$. In other words, by (29) and this last equation we have

$$F\chi(x) = F\chi(1)\,\bar{\chi}(x).$$

Thus if χ is a primitive character $\bmod A$

$$F\chi = (F\chi(1))\bar{\chi}.$$

When χ is a primitive character $\bmod A$ we denote $F\chi$ simply $\hat{\chi}$; thus $\hat{\chi} = \hat{\chi}(1)\bar{\chi}$. Similarly if α is a primitive character $\bmod M$, $\hat{\alpha}$ denotes $F_M \alpha$ and so $\hat{\alpha} = \hat{\alpha}(1)\bar{\alpha}$. Now let χ be any character $\bmod A$, $M = M(\chi)$ its conductor

and α its primitive. Let $\{W_D\alpha\}$ be the basis of $L_\chi(A)$ constructed in Theorem 3. Then $F_A W_D = F_A I_A^{MD} J_{MD}^M = J_A^{MD} F_{MD} J_{MD}^M = J_A^{MD} I_{MD}^M F_M$, by a double application of Theorem 5. But by Theorem 2(c), $J_A^{MD} I_{MD}^M = I_A^C J_C^M$, where $C = AM/MD = M \cdot (A/(MD)) = MD'$. Here $D' = A/MD$ is the complementary divisor to D of A/M, i.e., $DD' = A/M$. Thus $F_A W_D = I_A^{MD'} J_{MD'}^M F_M = W_{D'} F_M$. In particular, with $F = F_A$, $F(W_D\alpha) = W_{D'}(F_M\alpha) = W_{D'}(\hat{\alpha}(1)\bar{\alpha}) = \hat{\alpha}(1)\, W_{D'}\bar{\alpha}$. Suppose χ is not real, then $M(\bar{\chi}) = M(\chi)$ and the primitive of $\bar{\chi}$ is $\bar{\alpha}$. Arrange a basis for $L_\chi \oplus L_{\bar{\chi}}$ by stronging together the $\tau(A/M)$ pairs of functions $W_D\alpha$, $W_{D'}\bar{\alpha}$; as D ranges over the divisors of A/M so does D' and $(D')' = D$. The action of F on such a pair as we have just seen is $F(W_D\alpha) = \hat{\alpha}(1)\, W_{D'}\bar{\alpha}$ and also $F(W_{D'}\bar{\alpha}) = \hat{\bar{\alpha}}(1)\, W_D\alpha$. A standard fact about the Fourier transform is $F(\bar{f})(x) = \overline{Ff(-x)}$, from which $\hat{\bar{\alpha}}(1) = \overline{\hat{\alpha}(-1)} = \overline{\hat{\alpha}(1)\,\alpha(-1)} = \alpha(-1)\,\overline{\hat{\alpha}(1)}$, since $\alpha(-1) = \pm 1$. The matrix of F on this pair is then

$$\begin{pmatrix} 0 & \alpha(-1)\,\overline{\hat{\alpha}(1)} \\ \hat{\alpha}(1) & 0 \end{pmatrix}$$

and the matrix of F on $L_\chi \oplus L_{\bar{\chi}}$ consists of $\tau(A/M(\chi))$ such blocks strung along the diagonal. In particular, the contribution of $L_\chi \oplus L_{\bar{\chi}}$ to trace F is 0.

If χ is real so is its primitive α, so $F(W_D\alpha) = \hat{\alpha}(1)\, W_{D'}\alpha$ and L_χ is mapped onto itself by F. If A/M is not a square then $D' \neq D$ for all divisors of A/M and the $\tau(A/M)$ functions $\{W_D\alpha\}$ may be grouped into $\frac{1}{2}\tau(A/M)$ pairs $W_D\alpha$, $W_{D'}\alpha$ and the matrix of F on L_χ is then seen to consist of $\frac{1}{2}\tau(A/M)$ blocks

$$\begin{pmatrix} 0 & \hat{\alpha}(1) \\ \hat{\alpha}(1) & 0 \end{pmatrix}.$$

If A/M is a square, $= B^2$, then $D = B$ is the unique divisor of A/M having $D' = D$. Then $F(W_B\alpha) = \hat{\alpha}(1)\, W_B\alpha$, $W_B\alpha$ is an eigenfunction of F with eigenvalue $\hat{\alpha}(1)$. Besides $W_B\alpha$ there remain $\tau(A/M) - 1$ functions, which as before can be arranged in $\frac{1}{2}(\tau(A/M) - 1)$ pairs affording the same 2×2 blocks down the diagonal. In particular, for χ real the contribution of L_χ to trace F is 0 except if $A/M(\chi)$ is a square, in which case the contribution is $\hat{\alpha}(1)$. Such χ's were called special. Thus

$$\text{trace } F = \sum_{\chi \text{ special}} \hat{\alpha}(1), \tag{30}$$

which may be compared with (28). For the case that $(A, 2) = 1$ we have seen that there is only one special character mod A, namely, that χ whose primitive is the Jacobi symbol $\alpha(x) = (x/M)$, M the square-free part of A. In this case the result appears—in a somewhat different form—in [1, Chap. 8]. If there are no special characters mod A then (30) gives trace $F = 0$.

REFERENCES

1. E. HECKE, "Vorlesungen über die Theorie der Algebraischen Zahlen" Chelsea, New York, 1948.
2. W. LEDERMANN, "Introduction to Group Characters," Cambridge Univ. Press, London 1977.
3. N. NAKAGOSHI, The structure of the multiplicative group of residue classes modulo P^{N+1}, *Nagoya Math.* **73** (1979), 41.
4. W. NARKIEWICZ, "Elementary and Analytic Theory of Algebraic Numbers," PWN-Polish Scientific Publishers, Warsaw, 1974.